12 DE FEBRERO DE 2024

POLÍTICA DE SEGURIDAD

SERGIO VIGIL DÍAZ

Índice de contenido

Objetivos o elementos a proteger

Datos de los clientes: Información personal, financiera o de contacto de los clientes de la empresa.

Propiedad intelectual: Información confidencial sobre productos, procesos o estrategias comerciales que la empresa llevará a cabo.

Infraestructura de TI: Servidores, redes y sistemas de almacenamiento que son fundamentales para el correcto funcionamiento de la empresa.

Cumplimiento de la normativa: La empresa debe cumplir con las regulaciones específicas relacionadas con la protección de datos y la seguridad de la información.

Riesgos concretos

Los ataques a los que se puede ver enfrentada la empresa pueden ser:

Ataque de acceso no autorizado: Un atacante intenta acceder a la información confidencial de clientes o datos internos de la empresa sin haberle concedido permiso, como datos de clientes, compras realizadas por los mismos, etc.

Ataque de denegación de servicio (DDoS): Un atacante intenta inundar el sitio web con tráfico falso para dejarlo inaccesible para que nadie pueda entrar a la página.

Phishing: Los atacantes envían correos electrónicos fraudulentos que pretenden ser la empresa de gominolas para engañar a los clientes y obtener información confidencial como contraseñas, tarjetas de crédito, etc.

Inyección de código SQL: Los atacantes introducen código SQL en alguna parte de la página para crear, leer, actualizar, modificar o eliminar datos de la base de datos de la empresa.

Mecanismos de seguridad a implantar

Para prevenir el acceso no autorizado, se deben de implementar medidas de autenticación fuertes, como contraseñas seguras y autenticación de dos factores.

Para los ataques DDoS, se pueden utilizar servicios de mitigación de DDoS que puedan detectar y filtrar el tráfico malicioso antes de que llegue a la página web. Además, también se puede preparar la web para que esté preparada para esos picos de usuarios.

Recordar a los clientes cómo identificar correos electrónicos de phishing y nunca solicitar información confidencial a través de correo electrónico.

Finalmente, para protegerme contra la inyección de código SQL, se pueden validar correctamente todos los datos de entrada en los formularios web y utilizar consultas parametrizadas y evitar la concatenación de cadenas.

Roles principales que intervendrán en la implantación y gestión de la política de seguridad

Director de seguridad de la información o CISCO: Es el responsable general de la política de seguridad de la empresa.

Equipo de seguridad de la información: Se encargan de implementar las medidas de seguridad y monitorear su eficacia.

Departamento de TI: Son los responsables de mantener la infraestructura tecnológica segura.

Personal de recursos humanos: Son los encargados de asegurar que los empleados estén informados y cumplan con las políticas de seguridad, entre otras cosas.

Normas del puesto de trabajo

1. **No compartir contraseñas con colegas o personas no autorizadas.** Las contraseñas son la primera línea de defensa contra accesos no autorizados a sistemas y datos confidenciales. Compartir contraseñas aumenta el riesgo de que los sistemas sean comprometidos. Cada empleado debe ser responsable de mantener su contraseña segura y confidencial.
2. **Bloquear la sesión cuando el puesto de trabajo quede desatendido.** El bloqueo de la sesión evita que personas no autorizadas accedan a los dispositivos y datos cuando un empleado no está presente en su puesto de trabajo. Esta medida ayuda a prevenir el acceso no autorizado y protege la privacidad y seguridad de la información.
3. **Actualizar regularmente el software y sistemas de seguridad.** Las actualizaciones de software y sistemas de seguridad suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas. Mantener el software actualizado es fundamental para proteger los sistemas contra ataques cibernéticos y garantizar su integridad y disponibilidad.
4. **No descargar software o archivos de fuentes no confiables.** Descargar software o archivos de fuentes no confiables aumenta el riesgo de infección por *malware* y otras amenazas cibernéticas. Solo se deben descargar y

ejecutar archivos de fuentes verificadas y seguras para garantizar la seguridad de los sistemas y datos de la empresa.

5. **Informar inmediatamente cualquier incidente de seguridad o sospecha de violación de seguridad.** La detección temprana y la respuesta rápida a incidentes de seguridad son fundamentales para minimizar el impacto de posibles violaciones de seguridad. Todos los empleados tienen la responsabilidad de informar de inmediato cualquier incidente o sospecha de violación de seguridad al departamento de seguridad de la información o al equipo designado para manejar tales eventos.